MINISTÈRE
DE LA JUSTICE
Liberté
Égalité
Fraternité

Politique Ministérielle de Sécurité Numérique

Version 2023-2024

Table des matières

1. Avant-propos

La transformation numérique, dans laquelle le ministère de la Justice est pleinement impliqué, accroit notre exposition au numérique. Dans un contexte où les menaces cyber sont protéiformes et en augmentation constante, les institutions publiques sont des cibles particulièrement exposées. Les menaces s'affranchissent des frontières, profitent des interdépendances des systèmes d'information et sont susceptibles d'impacter toute une institution.

Aussi, la sécurité numérique est une condition fondamentale pour répondre aux enjeux de la transformation numérique et des missions du service public de la Justice.

L'État répond à l'évolution des menaces et aux enjeux. Il déploie un dispositif d'ensemble qui se traduit notamment par une organisation de la gouvernance de la sécurité numérique, de la maîtrise du risque numérique et de la gestion des incidents de sécurité.

La présente politique ministérielle de sécurité du numérique décline pour le ministère de la Justice les moyens mis en œuvre dans ce domaine.

2. Champ d'application

2.1. Cadre légal

Le présent document définit la politique ministérielle de sécurité numérique du ministère de la justice (PMSN-MJ).

La PMSN vient décliner l'instruction générale interministérielle (IGI) n°1337/SGDSN/ANSSI du 26 octobre 2022 portant sur l'organisation de la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics. Cette politique prend en compte les spécificités du ministère de la justice et son organisation.

La PMSN s'adresse à l'ensemble des services du ministère et des établissements publics placés sous sa tutelle.

La PMSN s'applique également, par voie contractuelle ou conventionnelle, aux gestions déléguées et aux services externalisés par le ministère de la justice (fournisseurs, prestataires de services, sous-traitants, etc.) ainsi qu'aux partenaires (organisations syndicales, mutuelles, associations, etc.) lorsqu'ils concourent aux missions du ministère ou qu'un accès aux informations du ministère leur a été accordé. L'ensemble de ces acteurs proches est appelé « écosystème numérique » du ministère de la Justice.

2.2. Corpus de la sécurité numérique du ministère de la justice

La PMSN est complétée par un corpus documentaire disponible en annexe. Le premier document recense l'ensemble des annexes et est le plan de numérotation. Les annexes sont regroupées par catégories thématiques afin de faciliter la mise à jour du corpus, les recherches et l'appropriation par les différents acteurs. Tous les acteurs définis au paragraphe 3.1 de la PMSN peuvent proposer de nouveaux documents et des évolutions.

Pour le compte de la Haute fonctionnaire défense et sécurité (HFDS), le Fonctionnaire de la sécurité des systèmes d'information (FSSI) maintient à jour la liste structurée des documents, de leur porteur, de leur publication et leurs actualisations. Il assure également la communication auprès de chaque entité concernée.

Afin de maintenir le corpus de la PMSN à l'état de l'art, de mettre en œuvre la feuille de route ministérielle et de répondre aux risques conjoncturels, le comité de pilotage de la sécurité numérique (COPIL-SN) peut temporairement produire de nouvelles annexes et apporter des modifications aux documents existants. Ces modifications ne peuvent en aucun cas porter atteinte au fonctionnement des services, modifier les modalités de gouvernance et les responsabilités des acteurs. Ces modifications doivent être approuvées par le comité stratégique de la sécurité numérique (COSTRA-SN) suivant.

2.3. Catégories thématiques des annexes

Catégorie A : Organisation et gestion des incidents cyber

Porteur : SHFD/FSSI : Responsable du CSIRT

Catégorie B : Démarche et homologation de sécurité

Porteur : SHFD/FSSI : Responsable du pilotage et du contrôle des risques numériques

Catégorie C : Contrôle et d'audit de sécurité

Porteur : SHFDS/FSSI : Responsable du pilotage et du contrôle des risques numériques

Catégorie D : Recrutement, formation et sensibilisation

Porteur : SHFD/FSSI : Responsable du CSIRT

Catégorie E : Déclinaisons directionnelles ou spécifiques de la PMSN

Porteur : Tous les acteurs du COPIL-SN

Catégorie F : Directives techniques

Porteur : SNUM : Responsable Central de la Sécurité des Système d'information

3. Organisation ministérielle de la gouvernance de la sécurité numérique

3.1. Chaînes, rôles et responsabilités

3.1.1. La chaîne décisionnelle de sécurité numérique

Afin de mener à bien ses missions, le garde des Sceaux, ministre de la justice, s'appuie sur une **chaîne décisionnelle** et sur des **instances de gouvernance** pour définir et contrôler la stratégie ministérielle de sécurité du numérique. Cette stratégie a pour objectif d'accompagner le plan de transformation numérique et de renforcer la résilience du ministère face aux cyberattaques.

Les rôles et responsabilités présentés ici sont issus de l'arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics. Cette section décline ces rôles dans le cadre du ministère de la Justice.

3.1.1.1. Le garde des Sceaux, ministre de la Justice

Le **garde des Sceaux est responsable de la sécurité numérique** des systèmes d'information et de communication du ministère et de ses établissements publics.

À ce titre, le ministre valide la politique ministérielle de sécurité numérique (PMSN), fixe les orientations stratégiques et s'assure que l'ensemble des systèmes d'information (SI) du ministère sont sous la responsabilité d'une autorité qualifiée en sécurité des SI (AQSSI) en charge de la **maîtrise des risques numériques**.

Le ministre **préside le comité stratégique de la sécurité numérique** pendant lequel la feuille de route et les amendements de la politique ministérielle de sécurité numérique sont approuvés.

3.1.1.2. Le haut fonctionnaire de défense et de sécurité

Le haut-fonctionnaire de défense et de sécurité (HFDS)(1) conseille le ministre pour toutes les questions relatives à la sécurité du numérique.

À ce titre, le HFDS **propose au ministre la politique ministérielle de sécurité numérique** qu'il est chargé d'animer.[1]

Le HFDS nomme un adjoint (HDFS-A) qui l'accompagne dans la réalisation de ses missions.

Le HFDS **préside le comité de pilotage de sécurité numérique**. À ce titre, le HFDS planifie et anime ce comité. Il peut décider de déléguer cette présidence au fonctionnaire de sécurité des systèmes d'information (FSSI).

[1] Article 4.2.2.1 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

3.1.1.3. Les autorités qualifiées en sécurité des systèmes d'information

L'autorité qualifiée en sécurité des systèmes d'information (AQSSI)[2] [3] est responsable de la sécurité des services numériques placés sous sa responsabilité et de leur homologation. Elle nomme, lorsqu'elle n'exerce pas elle-même cette fonction, des autorités d'homologation (AH) qui sont alors chargées après instruction du dossier d'homologation, de prononcer l'homologation. Cette nomination ne décharge pas l'AQSSI de ses responsabilités.

L'AQSSI réalise de plusieurs missions :

- Garantir les ressources nécessaires pour mener à bien les projets de transformation numérique de son périmètre et **s'assurer que les risques numériques sont connus et maîtrisés.**
- Réaliser et tenir à disposition du HFDS la **cartographie des risques numériques et des partenaires essentiels** à son activité.
- **Contribuer à l'élaboration du rapport annuel de sécurité numérique** qui intègre l'évaluation du niveau de risque de chaque direction et la synthèse des incidents de sécurité numérique pour le ministère. Ce rapport est présenté en comité stratégique de la sécurité numérique.
- **Participer à la résilience du ministère par l'élaboration et la mise en œuvre des plans de continuité d'activité** pour faire face à des incidents de sécurité numérique.
- S'assurer au travers d'exercices de la connaissance, de la **maîtrise des plans de reprise et de continuité d'activité, et de leur mise à jour**.

En cas d'incident numérique « très grave » pour le fonctionnement du ministère, les AQSSI sont intégrés à la cellule de crise ministérielle.

Sont désignés « autorités qualifiées en sécurité des systèmes d'information »[4] :

- Les directeurs des administrations centrales,
- Les chefs de service à compétence nationale rattachés directement au ministre ou à caractère interministériel,
- Les directeurs des établissements publics de l'État.

L'AQSSI préside le comité de gestion des risques numériques de sa structure.

[La nomination d'AQSSI des services déconcentrés sera précisée dans une version ultérieure de cette politique de sécurité numérique.]

[2] Article 4.2 du décret n° 2019-1088 du 25 octobre 2019
[3] Article 4.2.3 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI
[4] Article 1 de l'Arrêté du 17 février 2020 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle du ministre de la Justice

3.1.1.4. Le chef du service numérique (SNUM)

Le chef du service du numérique ministériel (SNUM)[5] définit la stratégie d'hébergement des services numériques et il s'assure de la prise en compte dans son service de la politique ministérielle de sécurité du numérique.

Le chef du SNUM assure la **mise en œuvre et l'exploitation de services numériques et d'infrastructures du ministère**.

A ce titre, pour les SI dont il a la charge, il veille :

- A l'élaboration et au maintien à jour d'une cartographie des systèmes d'information sous sa responsabilité ;
- Au maintien en condition opérationnelle et de sécurité des SI ;
- A la résilience numérique des services dont il a la charge ;
- A l'élaboration et la mise en œuvre des plans de continuité et de reprise informatique ;
- A la fourniture de moyens permettant de prévenir et de répondre aux incidents d'origine cyber.

Le chef du service numérique est **AQSSI du socle technique.** Ce socle est composé des briques d'infrastructure et des services mutualisés. A ce titre, il procède à l'homologation de sécurité de ces SI. Le FSSI et les CSN des directions utilisatrices de ses services mutualisés sont membres de droit de la commission d'homologation.

3.1.2. La chaîne fonctionnelle de sécurité numérique

Afin de mener à bien ses missions, le ministère s'appuie sur une **chaîne fonctionnelle dédiée** et sur des **instances de pilotage** qui permettent de concilier les instances décisionnelles et les instances opérationnelles. Cette chaîne a la charge du **pilotage et du contrôle de la mise en œuvre opérationnelle** de la stratégie de sécurité numérique.

Les rôles et responsabilités présentés ici sont issus de l'arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics. Cette section décline ces rôles dans le cadre du ministère de la Justice.

3.1.2.1. Le fonctionnaire de sécurité des systèmes d'information

Le fonctionnaire de sécurité des systèmes d'information (FSSI)[6] [7] pilote la mise en œuvre de la politique ministérielle permettant de maîtriser les risques de sécurité du numérique, de garantir la continuité des activités et la résilience du ministère. Il est consulté sur la bonne prise en compte de la sécurité du numérique dans les politiques publiques du ministère, la stratégie ministérielle du numérique et leurs déclinaisons au sein des directions.

[5] Article 4.2.5 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI
[6] Article 4.1 du décret n° 2019-1088 du 25 octobre 2019
[7] Article 4.2.2.2 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

Le FSSI réalise plusieurs missions :

- **Conseiller et accompagner** l'ensemble des acteurs du ministère ainsi que les établissements publics sur les questions relatives à la sécurité du numérique.
- **S'assurer de la cohérence globale des mesures** en matière de sécurité numérique et de la prise en compte, au sein du ministère et des établissements publics, du respect des règles et des orientations politiques en matière de sécurité numérique.
- **Contrôler** l'application des exigences de sécurité définies dans le présent document et ses annexes à l'aide d'audits, de contrôles et de bilans.
- **Produire un avis formel sur les dossiers de sécurité** des systèmes d'information d'importance vitale (SIIV) et des systèmes d'information essentiels (SIE) dans le cadre de ses missions de conseil auprès des AQSSI.

Le **FSSI pilote la réponse aux incidents « très grave ».** À ce titre, il s'appuie sur le CSIRT ministériel placé sous son autorité.

Il informe l'agence nationale de sécurité des systèmes d'information (ANSSI) des incidents « grave » et « très grave » sur les systèmes d'information et de communication du ministère et des organismes placés sous sa tutelle.

Le FSSI est nommé par arrêté ministériel.

Le FSSI assure le secrétariat du comité de pilotage de la sécurité numérique. Du fait de la délégation du HFDS, il assure aussi la présidence.

Le FSSI préside le comité technique de sécurité des systèmes d'information (COTEC-SSI).

3.1.2.2. Les conseillers à la sécurité du numérique (CSN)

Le **conseiller à la sécurité du numérique** (CSN)[8] conseille et accompagne l'autorité qualifiée en sécurité des systèmes d'information dans l'exercice de ses responsabilités **pour la gestion des risques numériques**, les démarches d'homologation, l'évaluation fonctionnelle des incidents numériques, **l'anticipation et le traitement des crises d'origine cyber.**

Le CSN réalise plusieurs missions :

- **Piloter la mise en œuvre des enjeux de sécurité** métier dans le cadre de la feuille de route ministérielle.
- **Conseille l'autorité qualifiée ou l'autorité d'homologation** pour l'homologation des systèmes d'information.
- **Suivre les plans d'action** décidés en commission d'homologation.
- Présenter le **niveau de sécurité** et les **risques liés à la sécurité numérique** des systèmes d'information de son entité.
- Informer l'autorité qualifiée en sécurité des systèmes d'information (AQSSI) lors du comité opérationnel de gestion des risques.

[8] Article 4.2.4 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

- Participer à la gestion des incidents « grave » et « très grave » pour évaluer les impacts métiers et informer sa chaîne décisionnelle.

Sans être un expert technique du domaine, il dispose d'une culture de la sécurité du numérique qui lui permet de traduire les enjeux en exigences de sécurité pour le compte de l'AQSSI.

Le **conseiller à la sécurité du numérique** (CSN) est nommé par note de service de son AQSSI et adressée au HFDS

Le CSN assure le secrétariat du comité de gestion des risques numériques de l'entité.

3.1.2.3. Les responsables centraux de la sécurité des systèmes d'information (RCSSI)

Les **responsables centraux de la sécurité des systèmes d'information** (RCSSI) sont les RSSI du **service numérique ministériel et des directions d'administration centrale**.

Les RCSSI réalisent plusieurs missions :

- **Garantir la mise en œuvre des moyens et des procédures techniques** en termes de sécurité numérique qui visent à répondre :
  - ➢ au plan de transformation numérique ministériel,
  - ➢ à la feuille de route ministérielle en matière de sécurité numérique,
  - ➢ aux enjeux de sécurité métier issus des analyses de risque.
- **Animer la communauté des RSSI** des services déconcentrés et des services à compétence nationale rattachés au service numérique ministériel ou aux directions d'administration centrale.

  • Piloter les incidents d'intensité « faible » à « modéré » dans le cadre d'un processus standard, maîtrisé et partagé et informer le responsable du CSIRT qui décide de partager les informations techniques afin d'anticiper les risques de propagation ou de latéralisation.

Dans le cadre des missions spécifiques au service numérique ministériel, le RCSSI doit :

- **Réaliser les missions d'un CSN auprès du chef du SNUM** dans le cadre de l'homologation du socle technique. Le socle est composé des briques d'infrastructure et des services mutualisés offert par le service numérique.
- Piloter et contrôler la réalisation des actions décidées en COTEC-SSI.
- Assurer le secrétariat du comité technique de sécurité des systèmes d'information (COTEC-SSI).

Les RCSSI sont nommés par note de service, publiée par l'AQSSI.

3.1.3. La chaîne opérationnelle de sécurité numérique et de cyberdéfense

Pour mener à bien ses missions, le ministère s'appuie sur une **chaîne opérationnelle dédiée** et sur des **instances de suivi** qui permettent de décliner de manière concrète et

pragmatique la stratégie ministérielle de sécurité numérique en recherchant l'efficience. En cas de difficulté, elle informe la chaîne fonctionnelle avant toute mise en œuvre ou modification des actions validées en COTEC-SSI, COPIL-SN ou cellule de crise ministérielle.

3.1.3.1. Le responsable du CSIRT ministériel

Le responsable du CSIRT ministériel est en charge de la veille cyber, de la préparation et de la réalisation d'exercices cyber, et du pilotage et de la réponse sur incident numérique « grave » et « très grave ». Il assure la bonne exécution des investigations et de la coordination des parties prenantes permettant de garantir une réponse efficace.

Le responsable du CSIRT réalise plusieurs missions :

- Piloter la veille sur les techniques d'attaques, les modes opératoires, les outils malveillants, les vulnérabilités logicielles, les marqueurs ou indices numériques. Cette veille permet de définir les schémas d'attaque, d'évaluer les risques, de proposer des mesures de prévention et d'enrichir les systèmes de détection.
- Assurer la réponse à incident de sécurité, pour lesquels il s'appuie sur le responsable du SOC ministériel (SNUM/B2SI/CRC) pour l'analyse des incidents de sécurités. Il est en charge des échanges avec les CSN des services impactés pour piloter la réponse organisationnelle. Il dispose de la délégation du FSSI pour informer l'ANSSI. Il a également la charge d'informer le délégué à la protection des données dans le cadre des déclarations à effectuer auprès de la CNIL et de préparer les dépôts de plainte auprès du parquet.
- Animer la chaîne de réponse à incident avec le responsable du SOC ministériel et des structures faisant l'objet d'une convention.
- Assurer la montée et le maintien en compétence des acteurs en charge de la réponse à incident.
- Organiser des exercices cyber pour tester les procédures de gestion des incidents.
- Sensibiliser les acteurs du ministère à la sécurité numérique.

Le responsable du CSIRT est nommé par note de service, publiée par le FSSI.

Le responsable du CSIRT est placé sous l'autorité hiérarchique du FSSI.

3.1.3.2. Le responsable SOC ministériel

Le responsable du SOC ministériel est responsable de la gestion technique des incidents de sécurité numérique.

Le Responsable du SOC Ministériel réalise plusieurs missions :

- Détecter, analyser et qualifier les évènements de sécurités numérique.
- Effectuer et organiser la veille sur vulnérabilité auprès des éditeurs de logiciel.
- **Assurer la gestion des incidents** des évènements de sécurité ayant un impact de **« faible » à « modéré »**.
- **Appuyer le CSIRT** dans le cas d'un **incident « grave » et « très grave »** survenant dans l'écosystème numérique du ministère.

Le responsable du SOC ministériel est nommé par note de service, publiée par le chef du service numérique ministériel.

Le responsable du SOC ministériel est placé sous l'autorité hiérarchique du RCSSI du service numérique ministériel.

3.1.3.3. Les responsables de la sécurité des systèmes d'information (RSSI)

Les responsables de la sécurité des systèmes d'information (RSSI) sont des **experts techniques** qui peuvent être affectés auprès :

- D'un CSN pour l'appuyer dans les domaines techniques propres à sa direction métier.
- D'un service à compétence nationale afin de traiter les spécificités de l'entité. Dans ce cadre, il rend compte au CSN de la direction de rattachement de l'avancement des travaux de la feuille de route ministérielle, et transmet les indicateurs de pilotage.
- D'une direction de programme afin de traiter les spécificités du projet. Dans ce cadre, il rend compte au CSN de la direction de rattachement de l'avancement des travaux de la feuille de route ministérielle, et transmet les indicateurs de pilotage.
- D'une structure numérique afin de maintenir, superviser, contrôler les systèmes locaux, piloter les actions validées en COTEC-SSI, opérer les actions d'endiguement et de remédiation en cas d'incident cyber.

Le RSSI est nommé par note de service, publiée par le responsable de l'entité.

Dans le cadre de la gestion des incidents, il réalise ou s'assure de l'exécution des prescriptions techniques du responsable du SOC ministériel. Il participe à la récupération et l'analyse des traces et informe les autorités de sa structure et son CSN de rattachement.

3.2. Les instances ministérielles

Pour mener à bien ses missions, le ministère s'appuie sur une comitologie à trois niveaux : **stratégique** pour la gouvernance, **pilotage** pour le suivi, **technique** pour la mise en œuvre opérationnelle.

Chacune de ces instances est composée comme suit :

- Un président, dont le rôle est de convoquer et d'animer le comité, et de valider le compte rendu proposé par le secrétaire ;
- Un secrétaire, dont le rôle est de formaliser le compte rendu du comité et de transmettre au président pour approbation avant diffusion à l'ensemble des parties prenantes ;
- Un ensemble d'acteurs, en fonction du comité ou de l'ordre du jour associé.

3.2.1. Le comité stratégique de la sécurité numérique

Le comité stratégique de la sécurité numérique (COSTRA-SN) valide les orientations stratégiques du ministère de la Justice en matière de sécurité du numérique. Il prend en compte les orientations du comité stratégique interministériel de la sécurité du numérique (COSINUS). Les membres du COSTRA-SN valident la feuille de route ministérielle pour répondre aux enjeux du ministère et aux décisions des réunions interministérielles cybersécurité (RIM cyber et COSINUS)[9].

Le comité stratégique de la sécurité numérique réalise plusieurs missions :

- Valider, amender et suivre l'avancement de la feuille de route ministérielle de sécurité numérique.
- Valider la politique ministérielle de sécurité numérique et ses annexes en s'appuyant sur les comptes rendus des comités de pilotage de la sécurité numérique.
- Valider la synthèse annuelle des incidents de sécurités qui sera transmise à l'ANSSI.

Le comité stratégique de la sécurité numérique est composé comme suit :

- Le ministre, en tant que président,
- Le Haut-fonctionnaire de défense et de sécurité,
- Le Haut-fonctionnaire de défense et de sécurité adjoint (HFDS-A) en tant que secrétaire,
- L'ensemble des autorités qualifiées en sécurité des systèmes d'information du ministère (AQSSI),
- Le fonctionnaire de sécurité des systèmes d'information,
- Toute personne ou expert nécessaire en fonction de l'ordre du jour.

Le comité stratégique de la sécurité numérique se réunit une fois par an sur convocation de son président.

3.2.2. Le comité de pilotage de la sécurité numérique

Le comité de pilotage de la sécurité numérique (COPIL-SN) a pour objectif de piloter les activités relatives à la sécurité numérique et d'assurer le suivi de la feuille de route validée lors du comité stratégique de la sécurité numérique**.** Il intègre les éléments du comité interministériel de pilotage de la sécurité numérique (CINUS)[10].

Le comité de pilotage sécurité du numérique réalise plusieurs missions :

- Piloter la feuille de route ministérielle de sécurité numérique.

[9] Article 3.3.1 et 3.3.2 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI
[10] Article 3.3.3 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

- Valider, amender jusqu'au prochain COSTRAT, les annexes à la PMSN permettant la mise en œuvre de la feuille de route.
- Prendre les décisions nécessaires au traitement des risques numériques sans remettre pas en cause le fonctionnement des activités essentielles et vitales du ministère.
- Décider des actions de contrôle en cas de constatation de dysfonctionnement, de non-respect de la PMSN ou de la feuille de route.
- Elaborer la synthèse des incidents de sécurité collectés auprès du comité technique de sécurité des systèmes d'information (COTEC-SSI).
- Préparer et proposer la feuille de route ministérielle.
- Alerter et sensibiliser la chaîne décisionnelle en cas de changement de l'état de la menace et de risques conjoncturels.
- Fixer les objectifs et priorités du COTEC-SSI.

Le comité de pilotage sécurité du numérique est composé comme suit :

- Le haut-fonctionnaire de défense et de sécurité (HFDS) et son adjoint en tant que président, représentés par le fonctionnaire de sécurité des systèmes d'information (FSSI),
- Le fonctionnaire de sécurité des systèmes d'information (FSSI) en tant que secrétaire,
- Les conseillers à la sécurité du numérique (CSN),
- Les responsables centraux à la sécurité des systèmes d'informations (RCSSI),
- Les RSSI de direction de programme,
- Le délégué à la protection des données,
- Toute personne ou expert nécessaire en fonction de l'ordre du jour.

Le comité de pilotage sécurité du numérique se réunit au minimum une fois tous les deux mois sur convocation de son président ou son représentant.

Les COPIL-SN font l'objet d'un compte rendu formel adressé à la chaîne décisionnelle.

3.2.3. Le comité technique de la sécurité des systèmes d'informations

Le comité technique de la sécurité des systèmes d'informations (COTEC-SSI) est responsable de la mise en œuvre des activités et chantiers relatifs à la sécurité du numérique, à la continuité d'activité et à la protection des données personnelles au sein de ses différentes directions.

Le comité technique de la sécurité des systèmes d'informations réalise plusieurs missions :

- Fixer les règles de sécurité et les mesures techniques à mettre en œuvre pour les atteindre.

- Piloter les plans d'actions associées.
- Suivre les chantiers validés par le comité de pilotage de la sécurité du numérique.

Le comité technique de la sécurité des systèmes d'informations est composé comme suit :

- Le fonctionnaire de sécurité des systèmes d'information (FSSI) en tant que président,
- Le responsable central de la sécurité des systèmes d'information (RCSSI) du SNUM, en tant que secrétaire,
- Toute personne ou expert nécessaire en fonction de l'ordre du jour.

Le comité technique de la sécurité des systèmes d'informations se réunit au minimum une fois par mois sur convocation de son président.

3.2.4. Le comité de gestion des risques numériques

Chaque entité placée sous la responsabilité d'une AQSSI organise **un comité de gestion des risques numériques.** Ce comité pilote la mise en œuvre des chantiers de sécurisation des SI de l'entité qui concourent à ses missions.

Le comité de gestion des risques numériques réalise plusieurs missions :

- Fournir à l'AQSSI une vision consolidée des risques numériques.
- Rendre compte de l'avancement des démarches de sécurité ses systèmes d'information.
- Vérifier la bonne exécution des plans d'actions sur lesquels l'AQSSI s'est engagée.
- Solliciter l'AQSSI en cas de difficultés dans l'exécution des plans d'actions et des démarches d'homologation.

Le comité de gestion de risque est composé comme suit :

- L'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI) en tant que président ;
- Le conseiller à la sécurité du numérique (CSN), en tant que secrétaire ;
- L'ensemble des autorités d'homologation (AH) désignées ;
- Les directions projets ;
- Toute personne ou expert jugée nécessaire au bon déroulement de l'ordre du jour.

Le comité de gestion des risques numériques se réunit au minimum deux fois par an sur convocation de son président ou par délégation du CSN.

4. Maîtrise du risque numérique

4.1. Typologie des systèmes d'information

La maitrise des risques numériques doit être adaptée aux enjeux de sécurité d'un système, notamment en fonction de leur criticité et de la nature des informations qu'il traite.

Afin de faciliter l'appréciation de la criticité et de la nature des informations traitées, le ministère de la justice met en œuvre les typologies suivantes.

Les systèmes d'information du ministère de la justice sont repartis en quatre catégories, de la criticité la plus faible à la plus forte.

Une note d'orientation, disponible dans le corpus de la sécurité numérique, permet d'apprécier la criticité des systèmes.

4.1.1. Les systèmes et services informatifs

Les systèmes et services informatifs ne sont destinés qu'à informer et à communiquer avec le public, qu'il soit interne au externe au ministère.

Ils ne concourent pas directement au fonctionnement ou à l'accomplissement de ses missions par le ministère, si bien qu'une atteinte portée à ces systèmes et services aurait un impact faible sur le fonctionnement et sur l'accomplissement de ses missions par le ministère.

Ils n'entraînent pas non plus d'échanges de flux de données entrant ou sortant avec le ministère.

Les besoins de sécurité de ces systèmes et services sont faibles.

4.1.2. Les systèmes d'information de gestion

Les systèmes d'information de gestion concourent, de manière accessoire au fonctionnement et à l'accomplissement de ses missions par le ministère.

Une atteinte portée à un système d'information de gestion aurait un impact modéré sur le fonctionnement et sur l'accomplissement de ses missions par le ministère.

Les besoins de sécurité des systèmes d'information de gestion sont modérés.

4.1.3. Les systèmes d'information essentiels (SIE)

Les systèmes d'information essentiels (SIE) sont identifiés par le ministère comme étant essentiels à son fonctionnement et à l'accomplissement de ses missions.

Une atteinte portée à un système d'information essentiel (SIE) aurait un impact grave sur le fonctionnement et sur l'accomplissement de ses missions par le ministère.

Les besoins de sécurité des systèmes d'information essentiels (SIE) sont importants. Afin de répondre à ces besoins de sécurité importants, ces systèmes doivent être conformes aux exigences de sécurité de la transposition en droit national de la directive NIS v2[11].

De plus, tout sous-système mutualisé utilisé par un système d'information d'importance vitale (SIIV), strictement nécessaire à son fonctionnement ou à sa sécurité, est identifié comme un système d'information essentiel (SIE).

4.1.4. Les systèmes d'information d'importance vitale (SIIV)

Les systèmes d'information d'importance vitale (SIIV) sont indispensables au fonctionnement et à l'accomplissement de ses missions par le ministère.

Une atteinte au fonctionnement ou la sécurité de ces systèmes aurait un impact très grave sur le fonctionnement et sur l'accomplissement de ses missions par le ministère et *« risquerait de diminuer d'une façon importante […] la sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population »*[12].

Les besoins de sécurité des systèmes d'information d'importance vitale (SIIV) sont très importants.

Ces systèmes sont soumis aux dispositions du Code de la défense, créées et modifiées par les lois de programmation militaire[13] (LPM) et doivent à ce titre faire l'objet de mesures de sécurité spécifiques.

Ces systèmes doivent être d'un des types prévus à l'annexe 3[14] de l'arrêté sectoriel « Activités judiciaires »[15] et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense.

La liste de ces systèmes est communiquée à l'agence nationale de la sécurité des systèmes d'information (ANSSI) annuellement et est protégée par le secret de la défense nationale.

4.2. Typologies des informations

[La catégorisation des informations au sein du ministère de la justice sera précisée dans la prochaine version de cette politique de sécurité numérique. Ce chantier est inscrit à la feuille de route 2023-2024 en lien avec les CSN des directions métiers.]

---

[11] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.
[12] Conformément aux dispositions de l'article L1332-6-1 du Code de la défense.
[13] LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale et LOI n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025.
[14] Annexe non publique en diffusion restreinte.
[15] Arrêté du 23 décembre 2021 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Activités judiciaires ».

4.3. Principes stratégiques de la maîtrise du risque numérique

4.3.1. Cartographies des risques numériques

La cartographie est un outil de pilotage indispensable à la maîtrise des risques numérique[16].

Le HFDS doit disposer d'une cartographie des risques numériques pesant sur le ministère à jour.

A cette fin, chaque entité placée sous l'autorité d'une AQSSI doit maintenir à jour un **inventaire des risques numériques et des partenaires essentiels** à son activité. L'autorité qualifiée en sécurité des systèmes d'information (AQSSI) est responsable de l'élaboration et du maintien à jour de la cartographie des risques numériques pesant sur son périmètre[17].

L'élaboration et le maintien à jour de la cartographie des risques numériques d'une entité est pilotée par le conseiller à la sécurité numérique (CSN) de l'entité.

La cartographie des risques numériques de chaque entité est alimentée par les éléments remontés par les responsables de projets, les SIC, et les audits réalisés.

Le conseiller à la sécurité numérique (CSN) rend compte à l'autorité qualifiée en sécurité des systèmes d'information (AQSSI) des risques importants pesant sur son entité au moins une fois par an et en cas de nouveaux risques jugés majeurs. Il informe systématiquement le fonctionnaire de sécurité des systèmes d'information (FSSI) des risques critiques impactant les systèmes d'information essentiels (SIE) et les systèmes d'information d'importance vitale (SIIV).

La cartographie des risques numériques de chaque entité alimente le rapport annuel sur la sécurité numérique du ministère.

4.3.2. Maîtrise des prestataires, fournisseurs et partenaires

Les autorités qualifiées en sécurité des systèmes d'information (AQSSI) s'assurent du traitement des risques que les activités des tiers (prestataires, fournisseurs ou partenaires) font peser sur le ministère. Lorsque les prestations intellectuelles ou techniques relèvent de différents directions ou services, une matrice validée par le donneur d'ordre doit être établi dans le but de définir les rôles et responsabilités des différentes parties prenantes.

Pour cela, les AQSSI veillent à insérer ou à faire insérer dans les contrats ou les conventions de service, des clauses de sécurité permettant l'engagement des tiers à répondre aux exigences de sécurité numérique du ministère. Ces exigences de sécurité se matérialisent par l'intégration d'un Plan d'assurance sécurité (PAS) au dispositif contractuel et doivent garantir la bonne exécution des prestations durant la durée du marché.

Ces clauses doivent notamment prévoir la faculté pour l'autorité qualifiée en sécurité des systèmes d'information (AQSSI), ou toute personne désignée par elle, de contrôler régulièrement le respect de ces exigences de sécurité.

---

[16] Se référer au guide pour la cartographie du système d'information, disponible sur le site de l'ANSSI.
[17] Art 4.2.3 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

Afin d'aider les entités du ministère à construire leurs exigences contractuelles, un modèle de Plan d'Assurance Sécurité (PAS) est proposé dans le corpus de la sécurité numérique.

4.3.3. Homologation de sécurité

Les infrastructures et services logiciels informatiques qui composent le système d'information et de communication de l'Etat, doivent faire l'objet de l'homologation de sécurité.[18]

La notion d'homologation de sécurité recouvre deux aspects :

- d'une part une démarche de maitrise des risques numériques ;
- d'autre part la décision formelle prise par l'autorité d'homologation à l'issue de la mise en œuvre de la démarche de sécurité.

4.3.3.1. Démarche d'homologation

La démarche d'homologation est la démarche de maitrise des risques numériques, destinée à identifier et traiter les risques liés à l'exploitation d'un système d'information.

La démarche d'homologation doit être adaptée aux enjeux de sécurité du système, notamment au contexte d'emploi, à la nature des données contenues, ainsi qu'aux utilisateurs.

La démarche d'homologation doit être initiée dès la phase de lancement du projet, être menée tout au long de son développement et doit permettre le suivi des risques numériques liés au système d'information après sa mise en production et tout au long de sa vie jusqu'à son retrait du service.

Dès le lancement du projet, la démarche d'homologation doit permettre de définir le périmètre, le cadre réglementaire applicable, les acteurs du projet ainsi que ses besoins de sécurité et typologies de SI.

Durant le développement du projet, la démarche d'homologation doit permettre de constituer un dossier de sécurité regroupant tous les documents permettant d'identifier les risques pesant sur le système d'information, les mesures prises pour traiter ces risques, et tout autre document attestant de la bonne prise en compte des exigences de sécurité dans le développement du projet. Ce dossier doit notamment comporter une analyse de risques, les besoins de sécurité du système d'information, les mesures de sécurité mises en œuvre, les rapports d'audits réalisés, les risques résiduels et les raisons justifiant leur acceptation.

Durant toute la durée de vie du système et jusqu'à son retrait du service, la démarche d'homologation doit permettre de s'assurer du suivi du plan d'action et du déploiement des mesures de traitement des risques. Ce suivi est effectué par un comité de gestion des risques directionnel, piloté par le CSN et présenté a minima annuellement à l'AQSSI de l'entité.

Un guide de l'homologation, disponible dans le corpus de la sécurité numérique détaille la manière dont doit être menée une démarche d'homologation.

[18] Article 3 du décret n° 2022-513 du 8 avril 2022

4.3.3.2. *Décision d'homologation*

L'homologation est également la décision formelle[19] par laquelle l'autorité d'homologation « *atteste que les risques pesant sur le système d'information ont été identifiés, que les mesures nécessaires pour le protéger sont mises en œuvre et que les risques résiduels ont été identifiés et acceptés* »[20].

L'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI), ou toute autorité d'homologation (AH) qu'elle désigne, prononce la décision d'homologation après avis de la commission d'homologation et du fonctionnaire de sécurité des systèmes d'information (FSSI) pour les systèmes d'information essentiels (SIE) et les systèmes d'information d'importance vitale (SIIV).

Cette décision fait l'objet d'une attestation formelle indiquant notamment le périmètre et la durée de l'homologation, les autorisations spécifiques liées au télétravail et les éventuelles réserves. Cette attestation est transmise au haut fonctionnaire de défense et de sécurité (HFDS).

Dans le cas d'une responsabilité partagée entre plusieurs autorités qualifiées pour la sécurité des systèmes d'information (AQSSI), les autorités qualifiées pour la sécurité des systèmes d'information s'accordent pour désigner une autorité d'homologation (AH) commune qui peut être l'une des AQSSI.

Une homologation de sécurité est obligatoire pour tous les systèmes d'information et est un prérequis indispensable à leur mise en service.

[19] Article 4.3 du décret n° 2019-1088 du 25 octobre 2019
[20] Arrêté sectoriel AJ, Annexe 1 ; 2. Règle relative à l'homologation.

5. La gestion des incidents de sécurité

5.1. Définitions

Un **incident de sécurité** est un événement qui perturbe ou altère le fonctionnement d'un service et dont la gravité peut porter atteinte aux missions du ministère et au bon fonctionnement de la justice. En fonction du degré de gravité sur l'organisation, l'incident peut être catégorisé de « simple » à « très grave » et nécessiter l'activation d'une cellule de crise.

La gestion des incidents a pour but de qualifier et de neutraliser les effets des incidents pour rétablir le service le plus rapidement possible et s'assurer que l'incident ne se reproduise pas.

5.2. Catégorie et gestion des incidents de sécurité

Le ministère doit qualifier les incidents de sécurité par niveau de gravité qui est fonction de l'impact sur le fonctionnement des services :

- **Faible** : Les services sont légèrement perturbés (perceptible, localisé), mais sans réel impact pour les activités du ministère, le fonctionnement d'une structure ou d'un établissement.
- **Modéré** : Le fonctionnement d'un service est perturbé (constaté, gène dans le fonctionnement), mais les impacts sont limités ou localisés. Ils ne portent pas atteinte de manière significative au bon fonctionnement de la structure ou de l'établissement.
- **Grave** : Les services sont perturbés au niveau national ou en ruptures au niveau local ou se propagent. Les structures locales rencontrent des difficultés sérieuses dans leur fonctionnement.
- **Très grave** : La conjonction de plusieurs incidents graves ou d'un incident majeur qui altère le fonctionnement des activités judiciaires, d'une zone de défense, d'un nombre important d'établissements, de l'ensemble des services d'une direction, d'un SIIV.

La gestion des incidents est pilotée à trois niveaux, en fonction de la gravité de l'incident :

- « Faible et Modéré » (incident contenu) : Pour les incidents d'intensité « faible » à « modéré », les RCSSI pilotent la gestion des incidents dans le cadre d'un processus standard et maîtrisé. Pour ce faire, ils s'appuient sur le responsable du SOC ministériel pour les SI d'information gérés par le SNUM ou sur des procédures de sécurité prévues dans les marchés pour les SI en gestion déléguée ou les SI externalisés. Pour les incidents « modérés », informe régulièrement et de façon transparente le FSSI, les CSN et le CSIRT. Le chef du SOC présente dans un rapport périodique, l'ensemble des incidents de sécurité traités sur la période.
- « Grave » : L'incident technique est piloté par le CSIRT. Le CSN et/ou le RCSSI concerné s'appuie sur les évènements remontés par le responsable du CSIRT pour analyser, évaluer les impacts fonctionnels et anticiper l'évolution de la situation. Il informe l'AQSSI qui décide, dans le cadre de la continuité d'activité, d'activer une cellule de crise directionnelle conformément à la politique de gestion de crise ministérielle.

- « Très grave » : Assisté du CSIRT, le FSSI pilote la gestion technique de l'incident. Il agit telle une cellule « situation » dédiée au numérique. Les CSN et les RCSSI participent aux points de situation et à l'élaboration des mesures qui seront proposés en cellule « décision » (direction de crise). La gestion des incidents « Très grave » s'inscrivent dans le processus de gestion de crise ministérielle qui est défini dans la politique dédiée.

Tous les incidents « grave » et « très grave » font l'objet d'un retour d'expérience (RETEX). Ce RETEX comprend un rappel des faits, l'évaluation des origines, des impacts, ainsi que le traitement de l'incident. Il intègre des recommandations et un plan d'actions afin de prévenir la survenance d'un incident similaire où d'en améliorer la gestion.

Le processus de gestion des incidents s'intègre dans la politique ministérielle de gestion de crise, mais également dans les politiques directionnelles de gestion de crise.

5.3. Déclaration des incidents à la CNIL

Tout incident, quelle que soit la gravité, fait l'objet d'un signalement circonstancié et détaillé au délégué à la protection des données (DPD) du ministère. Ce signalement est initié par le responsable du CSIRT et complété par les CSN des entités impactées.

Seul le DPD et ses équipes sont en capacité d'estimer la nécessité de déclarer l'incident à la CNIL et d'opérer cette déclaration[21].

[21] Article 33 du règlement (UE) 2016/679 dit RGPD

6. Cas particulier des établissements publics de l'Etat

Les établissements publics de l'État disposent d'une autonomie administrative et financière afin de remplir une mission d'intérêt général, précisément définie, sous le contrôle de l'État.

Le dirigeant exécutif de l'établissement est responsable, sur son périmètre, de la sécurité numérique. Cette[22] responsabilité se traduit par les exigences suivantes[23].

Le dirigeant exécutif est AQSSI sur son périmètre[24]. À ce titre, il est responsable de la sécurité numérique de l'ensemble de ses systèmes d'information et de l'homologation des systèmes d'information de son périmètre. Afin de mettre en place cette sécurité, le dirigeant exécutif de l'établissement peut se rapprocher du CSIRT ministériel(3).

Le dirigeant exécutif doit **désigner un point de contact direct pour le FSSI et le responsable du CSIRT ministériel.** Celui-ci peut être le responsable de la sécurité des systèmes d'information (RSSI) ou à défaut le directeur des systèmes d'information (DSI) de l'établissement[25].

Le dirigeant exécutif contribue à l'élaboration d'un rapport annuel de sécurité intégrant l'évaluation du niveau de sécurité du numérique et une synthèse des incidents de sécurité numérique. Ce rapport est partagé au FSSI annuellement[26].

Les incidents de sécurité affectant le système d'information et de communication de l'établissement doivent être déclarés auprès du FSSI du ministère, ainsi qu'à l'agence nationale de la sécurité des systèmes d'information (ANSSI) conformément à la IGI 1337.

[22] Article 4.4 du décret n° 2019-1088 du 25 octobre 2019
[23] Article 5 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI
[24] Article 2 de l'Arrêté du 17 février 2020 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle du ministre de la Justice
[25] Article 5.2 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI
[26] Article 5.3 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

7. Glossaire

Autorité d'homologation : personne physique qui, après instruction du dossier d'homologation, prononce l'homologation de sécurité du système d'information et de communication, c'est-à-dire, prend la décision d'accepter les risques résiduels identifiés sur le système.

Incident de sécurité : événement qui perturbe le fonctionnement d'un service et altère l'activité. En fonction de son degré de gravité et de son risque sur l'organisation, il peut être catégorisé de simple à majeur et nécessiter l'activation de la cellule de crise.

Plan de transformation numérique : document qui définit les orientations en matière de transformation numérique d'un ministère ou d'un établissement.

Politique de sécurité numérique : document qui définit les orientations en matière de sécurité numérique d'un ministère ou d'un établissement.

Résilience numérique : la résilience numérique désigne la capacité d'une organisation à mettre en place les moyens opérationnels adaptés aux menaces et les déployer pour, en cas de crise, être en mesure de maintenir et rétablir les services rendus par les systèmes d'information et de communication concourant à la réalisation des activités critiques de l'organisation, qu'ils soient internes ou externes.

Sécurité numérique : ensemble d'activités organisationnelles, techniques ou juridiques visant à protéger et défendre les systèmes d'information et de communication, ainsi que les informations qu'ils manipulent, contre d'éventuels incidents de sécurité de nature accidentelle ou intentionnelle, et à assurer la résilience numérique des entités concernées.

Système d'information et de communication de l'Etat : défini à l'article 1er du décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique, « [l]e système d'information et de communication de l'Etat est composé de l'ensemble des infrastructures et services logiciels informatiques permettant de collecter, traiter, transmettre et stocker sous forme numérique les données qui concourent aux missions des services de l'Etat et des organismes placés sous sa tutelle. »

Système d'information et de communication : sous-ensemble du système d'information et de communication de l'Etat mis en œuvre par une direction ou un service d'un ministère ou par un établissement public de l'Etat pour la réalisation de ses missions.

8. Références

(1) *Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics*

(2) *Arrêté du 17 février 2020 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle du ministre de la Justice*

(3) *Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique*

(4) *Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics*

(5) *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données.*